UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The Person of ALAN DANIEL GODOY GOMEZ	))))))))	Case No. 2:23-mj-00662-DUTY

FILED
CLERK, U.S. DISTRICT COURT
02/10/2023
CENTRAL DISTRICT OF CALIFORNIA
BY: GR DEPUTY

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-3

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 952	Importation of controlled substances
21 U.S.C. § 841(a)(1)	Possession with intent to distribute controlled substances
21 U.S.C. § 846	Conspiracy and attempt to distribute controlled substances

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Storm Rakela

Applicant's signature

HSI Special Agent Storm Rakela
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: Feb. 10, 2023

Karen L. Stevenson
Judge's signature

City and state: Los Angeles, CA

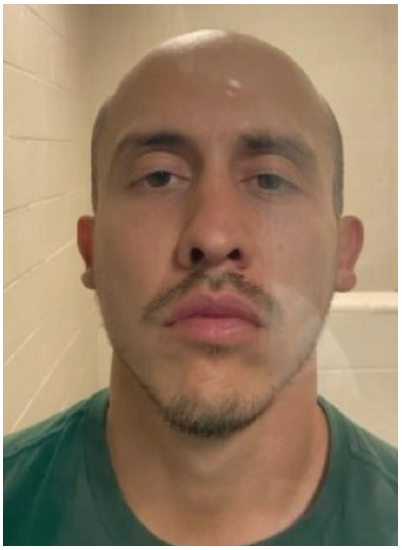
Karen L. Stevenson U.S. Magistrate Judge
Printed name and title

AUSA: LAURA A. ALEXANDER

ATTACHMENT A-3

PERSON TO BE SEARCHED

The person to be searched is identified as Alan Daniel GODOY Gomez, date of birth April 4, 1992. The search of GODOY shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within GODOY's immediate vicinity and control at the location where the search warrant is executed.



ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 952 (importation of controlled substances); 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances)(the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or

transferring money over $1,000, such as bank account records, cryptocurrency records and accounts;

e. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

f. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

g. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook,

Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

i. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

j. Contents of any calendar or date book;

k. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

l. Items, records or documents indicating ownership or occupancy over the SUBJECT PREMISES or the SUBJECT VEHICLE.

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as

viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be

seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

1. During the execution of this search warrant, law enforcement is permitted to: (1) depress both Alan Daniel GODOY Gomez's and Sergio Adan MONTOYA Hernandez's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Alan Daniel GODOY Gomez's and Sergio Adan MONTOYA Hernandez's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Storm Rakela, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search:

a. A 2018 grey Hyundai Tucson with Mexican license plate number AVR 642 A and Vehicle Identification Number ("VIN") TMCJ23A35HJ158537 ("SUBJECT VEHICLE 1"), as described further in Attachment A-1;

b. The residence located at 12135 Downey Avenue Unit D Downey, California 90241 (the "SUBJECT PREMISES"), as described further in Attachment A-2;

c. The person of Alan Daniel GODOY Gomez ("GODOY"), as described further in Attachment A-3;

d. The person of Sergio Adan MONTOYA Hernandez ("MONTOYA"), as described further in Attachment A-4; and

e. A 2015 white Nissan Sentra with California license plate number 8TOS221 and VIN 3N1AB7AP0FL634958 ("SUBJECT VEHICLE 2"), as described further in Attachment A-5.

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 952 (importation of controlled substances); 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, A-4, A-5 and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent ("SA") with Homeland Security Investigations (HSI) and have been so employed since September 2017. I am currently assigned to the Office of the Special Agent in Charge in Los Angeles, California, Border Enforcement Security Taskforce ("BEST") Los Angeles Metropolitan Group, and the Los Angeles Interagency Metropolitan Police Apprehension Crime Task Force ("LA IMPACT") Group 24 and have been so assigned since June 2021. I have over 24 years of law enforcement experience. I was a United States Border Patrol ("USBP") agent for approximately six years before my employment with HSI. For three of those six years, I was a Task Force Officer with the San Diego USBP Smuggling Interdiction Group ("SIG")/Drug Enforcement Administration ("DEA") Title 21 Group. Prior to my employment with the Department of Homeland Security ("DHS"), I was a Deputy Sheriff for over eleven years for the counties of Sacramento and San Diego in California. I have a

Bachelor of Science degree in Psychology from the University of California at Davis, California.

5. During my employment as a law enforcement officer, I have received training regarding laws pertaining to arrest, search and seizure, and evidence collection. I have also gained practical experience making arrests, conducting searches and seizures, and collecting evidence. This experience spans four different law enforcement agencies with established training programs.

6. Additionally, I have had hundreds of hours of formal and informal training in a wide variety of investigative and other law enforcement subjects, including mobile surveillance and narcotics sales and trafficking investigations. I have received numerous hours of instruction from federal agents, detectives, and other law enforcement officers regarding narcotics packaging, sales, transportation, and usage. I have received training from court-qualified experts in the fields of gangs, organized crime, general crimes, and narcotics-related investigations.

7. I have received specialized training in the fields of criminal investigation by attending numerous courses in criminal law, criminal investigation, narcotics investigation, and laws of arrest. I have attended surveillance courses, which included mobile and static surveillance. The class also covered counter-surveillance tactics utilized by criminals. I have conducted covert surveillance on residences, vehicles, and individuals that are suspected of selling narcotics. During these

operations, I have observed individuals use vehicles to smuggle controlled substances into the United States. I also conducted surveillance on vehicles transporting controlled substances and bulk cash within the United States. I have seen individuals use their own personal vehicles, borrow vehicles, or receive vehicles to transport illicit contraband.

8. I have assisted in serving search warrants for DHS, the Drug Enforcement Administration ("DEA"), the Federal Bureau of Investigation ("FBI"), the California Department of Justice ("CA DOJ"), LA IMPACT, and local police departments, in connection with investigations regarding narcotics, weapons, and various other offenses. I have had specialized training and field experiences in violations dealing with fentanyl, heroin, cocaine, amphetamines, cannabis, depressants, prescription medication, and other dangerous drugs.

III. SUMMARY OF PROBABLE CAUSE

9. As detailed below, on February 9, 2023, U.S. Customs and Border Protection ("CBP") screened SUBJECT VEHICLE 1 at the San Ysidro Port of Entry from Mexico in San Diego, California. The driver and only occupant of this vehicle was GODOY. At the primary inspection area, a CBP Officer's ("CBPO") certified drug detection dog screened and positively alerted to SUBJECT VEHICLE 1.

10. A CBPO scanned SUBJECT VEHICLE 1 with a Z-Portal x-ray machine. The CBPO observed anomalies within the center of the dashboard area of SUBJECT VEHICLE 1.

11. CBPOs and investigators on scene conducted a physical inspection of the dashboard area of SUBJECT VEHICLE 1 and observed packages contained therein consistent with known methods of smuggling bulk amounts of illegal drugs from Mexico into the United States.

12. Investigators in the Southern District of California did not alert the driver of the car to their discovery and instead obtained a tracker warrant for SUBJECT VEHICLE 1. HSI and local law enforcement conducted aerial and ground surveillance of SUBJECT VEHICLE 1 as it made its way up Interstate 5 from San Diego County to Los Angeles County.

13. At approximately 4:00 p.m., GODOY parked and exited SUBJECT VEHICLE 1 in a T.J. Maxx parking lot at 9050 Apollo Way Downey, California 90242. HSI SA Art Becerra saw MONTOYA enter SUBJECT VEHICLE 1 about ten minutes later. Law enforcement officers followed MONTOYA as he drove SUBJECT VEHICLE 1 to the SUBJECT PREMISES.

14. At approximately 5:11 p.m., law enforcement officers saw SUBJECT VEHICLE 1 exit the SUBJECT PREMISES. SUBJECT VEHICLE 1 drove towards the intersection of Alameda Street and Downey Avenue. Officer Jason Salazar of Culver City Police Department conducted a traffic stop of SUBJECT VEHICLE 1 near the intersection of Alameda Street and Brookshire Avenue. MONTOYA did not have a California driver's license and could not remember where he lived. Officer Salazar received verbal consent from MONTOYA for his certified drug detection dog to "sniff" SUBJECT VEHICLE 1. Officer Salazar's drug detection dog

gave a positive alert to the dashboard area of SUBJECT VEHICLE 1. Officer Salazar searched the dashboard area but did not find any controlled substances. MONTOYA had on his person two cell phones, a garage door remote control, and a set of keys with a vehicle fob. Officer Salazar found the keys and fob to SUBJECT VEHICLE 1 inside SUBJECT VEHICLE 1 and not on MONTOYA's person.

15. Law enforcement took the garage door remote control back to the SUBJECT PREMISES. They hit the button and apartment D's garage door opened. Law enforcement officers and agents entered the SUBJECT PREMISES in order to conduct a safety sweep and freeze the location pending this application for a search warrant. For their safety, they conducted a preliminary sweep of the SUBJECT PREMISES for any additional persons. They found no additional people at the SUBJECT PREMISES.

16. While conducting the safety sweep, law enforcement officers saw several bundles with black tape in a cardboard box on the bedroom floor of the SUBJECT PREMISES. Based on their training and experience, these officers believed the bundles looked like other bundles they have seized and later tested positive for controlled substances.

17. Law enforcement took the vehicle keys and fob they found on MONTOYA's person back to the T.J. Maxx parking lot. They used the vehicle fob to identify the vehicle MONTOYA drove to T.J. Maxx. This vehicle, SUBJECT VEHICLE 2, was a 2015 white Nissan Sentra with California license plate number 8TOS221.

IV. STATEMENT OF PROBABLE CAUSE

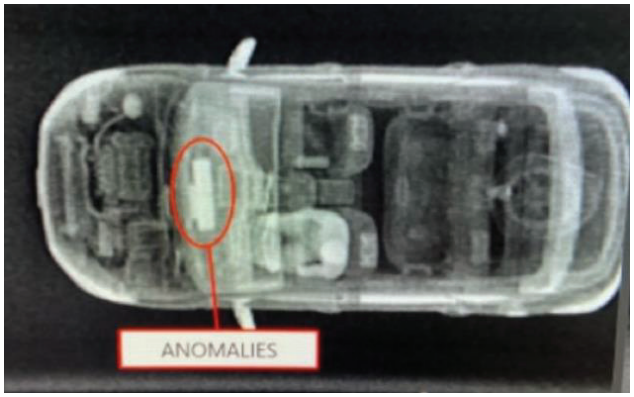
18. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. HSI INVESTIGATORS IDENTIFY SUBJECT VEHICLE 1 CONTAINING SUSPECTED NARCOTICS AT THE SAN YSIDRO PORT OF ENTRY

19. on February 9, 2023, U.S. Customs and Border Protection ("CBP") screened SUBJECT VEHICLE 1 at the San Ysidro Port of Entry from Mexico in San Diego, California. The driver and sole occupant of this vehicle was GODOY. At the primary inspection area, a CBPO's certified drug detection dog screened and positively alerted to SUBJECT VEHICLE 1.

20. The CBPO directed GODOY to the secondary inspection area. There, another CBPO asked GODOY to exit the vehicle and escorted him to a security office, out of view of the secondary inspection area.

21. In the secondary inspection area, an X-ray image of the vehicle with the Z-Portal x-ray machine revealed anomalies inside of the center of the dashboard area.



22. A CBPO officer searched the vehicle for about 10 minutes and found several wrapped packages, which appeared to contain a white powdery substance, hidden behind the center of the dashboard area.

23. CBPOs and investigators on scene conducted a physical inspection of the center of the dashboard area and observed packages contained therein consistent with known methods of smuggling bulk amounts of illegal drugs from Mexico into the United States.

24. Based on training and experience, including having found packages similarly concealed in vehicles many times in the past which proved to contain drugs after field and lab testing, officers and agents believe the packages contained prohibited drugs.

25. To facilitate further investigation, the packages were left in place and not opened or inspected and the driver was not alerted to the discovery. Investigators decided to try to follow SUBJECT VEHICLE 1 to its intended destination.

26. Because of the exigencies of the situation and to avoid a longer delay which might cause the driver or any co-conspirators to suspect or detect that the packages had been discovered by law enforcement, investigators installed a GPS tracking device on the SUBJECT VEHICLE 1 at approximately 12:01 p.m., so SUBJECT VEHICLE 1 and GODOY could leave the San Ysidro Port of Entry and continue to their intended destination. The tracking device was initially left in a mode that did not update or record location information, so that investigators could then

obtain a tracking warrant for SUBJECT VEHICLE 1. Investigators then began surveilling SUBJECT VEHICLE 1 unaided by the tracking device.

27. At approximately 1:05 p.m., investigators obtained a warrant authorizing the use of a tracking device on SUBJECT VEHICLE 1, signed by the Honorable Michael S Berg, U.S. Magistrate Judge for the United States District Court for the Southern District California.

B. SURVEILLANCE OF SUBJECT VEHICLE 1

28. Agents from HSI San Diego, along with detectives from LA IMPACT, Culver City Police Department, and other agencies, conducted surveillance of SUBJECT VEHICLE 1 driving along Interstate 5 from San Diego County to Los Angeles County.

29. At approximately 2:12 p.m., SUBJECT VEHICLE 1 exited Interstate 5 at Lakewood Boulevard in Downey, California. At approximately 2:32 p.m., SUBJECT VEHICLE 1 parked in front of a residence on 11th street in Downey, California 90241. GODOY waited about 45 minutes inside SUBJECT VEHICLE 1 until a black Toyota Corolla with California plate 7LKD152 arrived. GODOY exited SUBJECT VEHICLE 1 and shook hands with the driver of the Toyota Corolla. Both GODOY and the driver then entered the residence on 11th Street.

30. At approximately 3:50 p.m., GODOY exited the 11th Street residence and got into SUBJECT VEHICLE 1. Law enforcement followed SUBJECT VEHICLE 1 to T.J. Maxx at 9050 Apollo Way Downey, California 90242. At approximately 4:00 p.m., GODOY parked SUBJECT VEHICLE 1 and entered the T.J. Maxx.

HSI SA Art Becerra saw an unknown Hispanic male with black hair wearing a black shirt and shorts, later identified as MONTOYA, walk up to and enter SUBJECT VEHICLE 1. SA Becerra believes MONTOYA entered SUBJECT VEHICLE 1 about ten minutes after GODOY left it. MONTOYA drove SUBJECT VEHICLE 1 to an apartment complex at 12135 Downey Avenue Downey California 90242 (the complex housing the "SUBJECT PREMISES").

31. At approximately 5:11 p.m., law enforcement officers saw SUBJECT VEHICLE 1 exit the SUBJECT PREMISES. SUBJECT VEHICLE 1 drove towards the intersection of Alameda Street and Downey Avenue. Officer Jason Salazar of Culver City Police Department saw an object hanging from the rear-view mirror of SUBJECT VEHICLE 1 that obstructed the driver's view. He conducted a traffic stop of SUBJECT VEHICLE 1 near the intersection of Alameda Street and Brookshire Avenue. Officer Salazar identified MONTOYA by his Mexican voter card. MONTOYA did not have a California driver's license and could not remember where he lived. Officer Salazar received verbal consent from MONTOYA to permit his certified drug detection dog to "sniff" SUBJECT VEHICLE 1. Officer Salazar's drug detection dog gave a positive alert to the dashboard of SUBJECT VEHICLE 1. Officer Salazar searched the dashboard area but did not find any controlled substances. MONTOYA had on his person two cell phones, a garage door remote control, and a set of keys with a vehicle fob. Officer Salazar found the keys and fob to SUBJECT VEHICLE 1 inside SUBJECT VEHICLE 1 and not on MONTOYA's person.

C. Investigation of the SUBJECT PREMISES

32. At approximate 5:30 p.m., law enforcement took the garage door remote control back to the SUBJECT PREMISES. They hit the button to confirm which unit the opener accessed, and apartment D's garage door opened. Law enforcement officers and agents then entered the SUBJECT PREMISES through the garage in order to conduct a protective sweep and freeze the SUBJECT PREMISES pending this search warrant application. For their safety, the officers conducted a preliminary sweep of the residence for any additional persons. They found no people at the SUBJECT PREMISES.

33. While conducting the safety sweep, law enforcement officers saw several bundles with black tape in a cardboard box on the bedroom floor of the SUBJECT PREMISES. Based on their training and experience, these officers believe the bundles look like other bundles they have seized and later tested positive for controlled substances.

34. At approximate 6:20 p.m., law enforcement took the vehicle keys and fob found on MONTOYA's person back to the T.J. Maxx parking lot. They used this vehicle fob to identify the vehicle MONTOYA drove to T.J. Maxx. This vehicle, SUBJECT VEHICLE 2, was a 2015 white Nissan Sentra with California license number 8TOS221.

35. Recent surveillance confirms that since SUBJECT VEHICLE 1 arrived at the SUBJECT PREMISES at approximately 4:35 p.m., no other vehicles or individuals entered or left the SUBJECT PREMISES.

36. The SUBJECT PREMISES is located 12135 Downey Avenue apartment D, Downey California 90241. This apartment complex had four units labelled "A through D." The building is painted white. The front door of this apartment is white with a white "D" imprinted on the door above the peephole. Unit D has a maroon awning over its front door. The garage is attached to the unit so entrance of the unit through the garage is possible.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

37. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residences and businesses. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residences and businesses, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate

on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

38. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[1] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such

(footnote cont'd on next page)

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat

---

as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

39. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult

to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

40. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the

opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress GODOY's and MONTOYA's thumbs and/or fingers on the device(s); and (2) hold the device(s) in front of GODOY's and MONTOYA's faces with their eyes open to activate the facial-, iris-, and/or retina-recognition feature.

41. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

//

VII. CONCLUSION

42. For all of the reasons described above, there is probable cause to believe that the items to be seized described in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found at or in SUBJECT PREMISES, the SUBJECT VEHICLES, and the persons of GODOY and MONTOYA, as described in Attachments A-1, A-2, A-3, A-4, and A-5, respectively.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 10th day of February, 2023.

Karen L. Stevenson

THE HONORABLE KAREN L. STEVENSON
UNITED STATES MAGISTRATE JUDGE